

Консультация для педагогов «Информационная безопасность»

В это, возможно, сложно поверить, но сегодня, в век информационных технологий, шанс попасться на удочку мошенников ничуть не меньше, чем раньше. И часто причиной тому служит незнание самими пользователями основных **правил безопасности**, а порой и просто низкая бдительность.

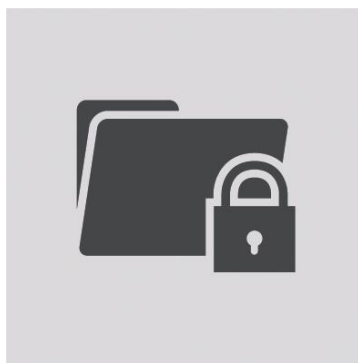
Например, попросили Вас предоставить все секретные данные вашей банковской карты при оплате товара через интернет, и вы сообщили конфиденциальную информацию. Либо установили «вирус» на свое мобильное устройство, перейдя по ссылке в SMS или в одном из популярных мессенджеров.

А потом в один прекрасный момент может оказаться, что деньги с вашей карты были списаны

Вы можете сказать, что такого никогда не случится, поскольку за безопасность отвечает банк. Отчасти это действительно так. Например, банк всегда использует инновационные технологии, обеспечивая безопасность своих клиентов.

Но, несмотря на меры, предпринимаемые банком, не нужно забывать о том, что безопасность должна соблюдаться, прежде всего, самими пользователями. Даже если вы уверены в том, что Вы знакомы со всеми правилами, не лишним будет еще раз повторить главные из них, чтобы не дать мошенникам шанс обмануть Вас.

Правило первое



Не сообщайте третьим лицам, включая сотрудников Банка, свои конфиденциальные данные: подтверждающие пароли, реквизиты банковской карты PIN и CVV-коды. Казалось бы, все об этом знают, но далеко не все применяют в жизни.

Важно знать: банк никогда не запрашивает пароль и не звонит клиенту для подтверждения отмены операции. Это еще одна уловка мошенников.

Правило второе



Используйте антивирус или установите приложение «****банк Онлайн» с бесплатным антивирусом для телефонов Android.

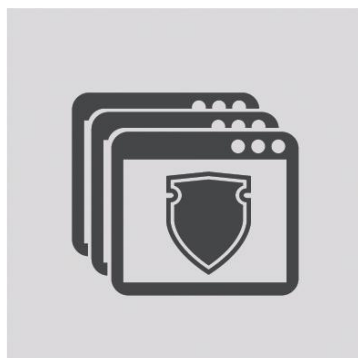
С информацией о мерах безопасности при использовании банковских карт, интернет-банка и мобильного приложения «****банк Онлайн» Вы можете ознакомиться [по ссылке](#).

Правило третье



Если Вы получили неожиданное сообщение по SMS или в одном из популярных мессенджеров или по электронной почте с предложением перейти по ссылке (например, по поводу объявления на каком-то сайте либо с ссылкой на фото), ни в коем случае не делайте этого

Правило четвертое



Скачивайте приложение «****банк Онлайн» только из официальных источников, таких как [GooglePlay](#), [AppStore](#), магазина [Windows](#).

Правило пятое



Если Вы вдруг потеряли мобильный телефон или сменили номер телефона, срочно обратитесь в контактный центр банка с просьбой заблокировать карту или уведомить банк о смене номера Вашего мобильного телефона.

Правило шестое



Не теряйте бдительность, внимательно проверяйте всю информацию о платеже, прописанную в SMS. Зачастую, пользуясь невнимательностью абонентов, мошенники просят подтвердить сторонние операции.

Конечно, шесть пунктов, указанных выше – это лишь часть всего свода правил, призванных обезопасить Вас от злоумышленников. Но, следуя хотя бы этим несложным предписаниям, Вы увеличите в разы эффект от усилий банка в области безопасности финансовых сервисов, и сделаете свою жизнь немного проще